WireGuard VPN 자체 구축

월정액 없는 나만의 VPN, VPS 한 대로 끝

OpenVPN vs WireGuard

OpenVPN

수십만 줄

코드 무겁고 설정 복잡 , 구형 표준

WireGuard

약 4 천 줄

커널 통합 · 가벼움 · 빠름 , 최신 암호 (ChaCha20)

키 페어 생성 순서

1. 서버에서 wg genkey → 서버 개인키 생성
2. wg pubkey 로 서버 공개키 추출
3. 클라이언트도 같은 과정으로 키 쌍 생성
4. 서로의 공개키만 교환 (개인키는 비공개)

서버 설정 wg0.conf

```
# /etc/wireguard/wg0.conf
[Interface]
PrivateKey = <SERVER_PRIVATE_KEY>
Address = 10.0.0.1/24
ListenPort = 51820
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT

# 방화벽 : UDP 51820 오픈
# ufw allow 51820/udp
```

클라이언트 peer 추가

- 서버 conf 에 [Peer] 블록 추가
- PublicKey = 클라이언트 공개키
- AllowedIPs = 10.0.0.2/32 (기기당 1 개 IP)
- 기기 추가 시마다 peer 블록 더 추가
- 기기 수 제한 없음 — WireGuard 의 장점

클라이언트 설정 파일

```
# client.conf
[Interface]
PrivateKey = <CLIENT_PRIVATE_KEY>
Address = 10.0.0.2/24
DNS = 1.1.1.1

[Peer]
PublicKey = <SERVER_PUBLIC_KEY>
Endpoint = SERVER_IP:51820
AllowedIPs = 0.0.0.0/0  # 전체 트래픽 VPN
PersistentKeepalive = 25
```

연결 테스트 + 문제 해결

- wg show 로 핸드셰이크 확인
- 클라이언트 → 10.0.0.1 핑으로 터널 검증
- 외부 사이트 핑으로 라우팅 정상 확인
- UDP 51820 방화벽 오픈 필수
- sysctl net.ipv4.ip_forward=1 (IP 포워딩)

kill switch + 운영 팁

- kill switch: 연결 끊기면 인터넷 차단
- PersistentKeepalive = 25 (NAT 환경 필수)
- 기기마다 이름 · 키 문서화
- 기기 분실 시 해당 키만 서버에서 삭제
- 다른 기기는 영향 없이 계속 연결

내 서버가 내 VPN 으로

🔗 Vultr $100 크레딧 (설명란)

🔗 WireGuard 전체 설정은 블로그에

🔗 구독 & 좋아요 부탁드려요

구독과 좋아요 부탁드립니다 ! 👍